REMARKS

The Examiner has rejected Claims 1-22 under 35 U.S.C. 102(b) as being anticipated by Conklin et al. (U.S. Patent No. 5,796,942). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to independent Claims 1, 8-10, 19, 20, 21, and 22, the Examiner has relied on the Summary and Col. 3, lines 37-43 in Conklin to make a prior art showing of applicant's claimed "establishing network communications with a plurality of computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity" (see the same or similar, but not necessarily identical language in each of the independent claims). Applicant respectfully asserts that Conklin only discloses an "Intrusion Detection portions of a Network Surveillance System." Applicant further notes that Figure 4 of Conklin shows a single intrusion detection block in communication with an operating system of a single computer, and not "a plurality of computers with firewalls," as specifically claimed by applicant.

Nevertheless, to further distinguish Conklin, applicant has amended the independent claims. See the highlighted claim language below, for example:

"(a) establishing network communications ~~with~~ between a server computer and a plurality of client computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity, and include a list of trusted and banned addresses;

(b) collecting the information from the firewalls of the client computers utilizing the network, for identifying similar intrusion activity across a subset of the plurality of client computers; and

(c) transmitting a response to the firewalls of ~~the~~ each of the plurality of client computers utilizing the network;

(d) wherein the firewalls are adapted for preventing the similar intrusion activity across each of the plurality of client computers utilizing the response" (see the same or similar, but not necessarily identical language in Claim 1 et al.)

"(a) establishing network communications ~~with~~ between a server computer and a plurality of client computers with firewalls over a network, wherein the firewalls are adapted for collecting information relating to intrusion activity, and include a list of trusted and banned addresses;

(b) collecting the information from the firewalls of the client computers utilizing the network;

(c) analyzing the information to ascertain intrusion activity including similar intrusion activity across a subset of the plurality of client computers;

(d) identifying a source of the ascertained intrusion activity; and

(e) notifying the source of the ascertained intrusion activity." (see the same or similar, but not necessarily identical language in Claim 10 et al.)

Applicant respectfully asserts that Conklin completely fails to teach client computers with firewalls, network communications "between a server computer and a plurality of client computers with firewalls," firewalls including "a list of trusted and banned addresses," and a technique for "identifying similar intrusion activity across a subset of the plurality of client computers," in the specific manner presently claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Conklin reference, especially in view of the amendments made hereinabove. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claim 4, the Examiner has relied on Col. 4, line 45-Col. 5, line 22 in Conklin to make a prior art showing of applicant's claimed technique "wherein the response includes the rules." Applicant respectfully asserts that Conklin simply teaches the Intrusion Detection [System] may incorporate algorithms or patterns to detect attempted intrusions. Thus, in Conklin, the intrusion detection system already has the rules such that it is unnecessary for "the response [transmitted to the firewalls to include] the rules," in the specific context claimed by applicant.

With respect to Claim 13, the Examiner has relied on the Summary; Col. 3, lines 3-11; and Col. 5, line 26-Col. 6, line 12 in Conklin to make a prior art showing of applicant's claimed technique "wherein the identification of the source further includes looking up an electronic-mail address based on the IP address." Applicant respectfully asserts that Conklin only teaches a source IP address, but does not specifically mention "looking up an electronic-mail address based on the IP address," as claimed by applicant (emphasis added).

With respect to Claim 17, the Examiner has relied on Col. 8, lines 1-24 in Conklin to make a prior art showing of applicant's claimed technique "wherein if it is determined that the response to the notification is not received, reporting the source of the intrusion activity to a central intrusion activity watch service." Applicant respectfully asserts that such excerpt merely discloses "provid[ing] an Alert Message." Applicant, on the other hand, specifically claims a "response to the notification" such that "if it is determined that the response to the notification is not received, the source of the intrusion activity [is

reported] to a central intrusion activity watch service" (emphasis added). Applicant emphasizes that Conklin only teaches sending an alert, but not any sort of response to the alert, and especially not in the specific context claimed by applicant.

Applicant again respectfully asserts that the Conklin reference fails to meet all of applicant's claim limitations, as noted above. Thus, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 23-29 below, which are added for full consideration:

"wherein the subset of the plurality of client computers includes a large subset of the plurality of client computers" (see Claim 23);

"wherein the similar intrusion activity includes a similar port scan performed across the subset of the plurality of client computers" (see Claim 24);

"wherein the similar intrusion activity includes an e-mail with a similar phrase sent across the subset of the plurality of client computers" (see Claim 25);

"wherein a user of each of the plurality of client computers is required to subscribe in order to track the collected information and confirm the collected information" (see Claim 26);

"wherein the collected information is included in a report according to categories of events" (see Claim 27);

"wherein additional information associated with the collected information is reported including a time and date of when the information was

collected, an Internet Protocol address associated with the collected information and applications associated with the collected information" (see Claim 28); and

"wherein the report is generated upon selection of a report icon in a graphical user interface" (see Claim 29).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P095/02.014.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100